УДК 003.26

ОПТИМИЗИРОВАННАЯ ПО ПАМЯТИ ЭЛЕКТРОННАЯ ПОДПИСЬ НА ОСНОВЕ СХЕМЫ ШТЕРНА С ПРИМЕНЕНИЕМ МОДИФИЦИРОВАННОГО ПРЕОБРАЗОВАНИЯ ФИАТА-ШАМИРА

Ниткин И.С. (ИТМО)

Научный руководитель – доктор технических наук, профессор ФБИТ Беззатеев С.В. (ИТМО)

Введение.

Современные криптографические алгоритмы, построенные на вычислительной сложности факторизации натурального числа, дискретного логарифмирования в конечном поле и извлечении квадратного корня в кольце вычетов по модулю составного числа потенциально уязвимы к атакам при помощи квантового компьютера [1]. Решением данной проблемы является разработка криптографических схем на основе вычислительных задач, решение которых за полиномиальное время не может быть получено с помощью квантового компьютера. Данный раздел криптографии (пост-квантовая криптография) является одним из наиболее востребованных в рамках современных исследований [2].

Схема Штерна [3] представляет собой протокол аутентификации без разглашения, построенный на вычислительной сложности решения NP-полной проблемы синдромного декодирования произвольного линейного кода. На основе протокола аутентификации без разглашения может быть разработана схема подписи при помощи преобразования Фиата-Шамира [4]. Такая электронная подпись представляет собой совокупность блоков обязательств и ответов схемы аутентификации без разглашения.

Основная часть.

Основным недостатком электронной подписи на основе схемы Штерна является значительный размер формируемой подписи.

В рамках исследования предложено использование модифицированного преобразования Фиата-Шамира. При проверке подписи на основе схемы Штерна для каждого раунда проверяются два из трех обязательств. Предложенная модификация предполагает размещение невостребованного обязательства в блоке ответов, при этом блок обязательств может быть уменьшен до размера одного значения хэш-функции.

Использование предложенной модификации позволяет сократить размер подписи на основе схемы Штерна. В рамках проведенных экспериментов установлено, что предложенная модификация также улучшает производительность алгоритма формирования подписи.

Криптографическая стойкость электронной подписи на основе схемы Штерна доказуемо сводится к сложности решения задач синдромного декодирования и поиска коллизии криптографической хэш-функции. Предложенная модификация не меняет структуру протокола аутентификации без разглашения, предложенного Штерном, поэтому никак не влияет на криптографическую стойкость схемы электронной подписи.

Заключение.

Таким образом, в рамках проведенного исследования предложены модифицированные алгоритмы формирования и проверки электронной подписи на основе схемы Штерна, произведена сравнительная оценка характеристик стандартной и модифицированной схем подписи, обоснована стойкость модифицированной схемы подписи на уровне стандартной схемы подписи на основе схемы Штерна.

Список использованных источников:

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring / P. W. Shor // Proceedings of the 35th Annual Symposium on Foundations of Computer Science : электронный журнал. – URL: https://doi.org/10.1109/SFCS.1994.365700.

2. Bernstein D.J. Introduction to post-quantum cryptography / D.J. Bernstein. – Berlin : Springer, 2009. – 248 с. – URL: https://doi.org/10.1007/978-3-540-88702-7_1 (дата обращения: 19.12.2022).

3. Stern J. A new identification scheme based on syndrome decoding / J. Stern // Advances in Cryptology — CRYPTO : электронный журнал. – URL: https://link.springer.com/content/pdf/10.1007/3-540-48329-2_2.pdf?pdf=inline%20link. – Дата публикации: 1993.

4. Fiat A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems / A. Fiat, A. Shamir // Advances in Cryptology — CRYPTO ’86 : электронный журнал. – URL: https://link.springer.com/content/pdf/10.1007/3-540-47721-7_12.pdf. – Дата публикации: 1986.